



2015 National Small Business Week



Tips for Managing the Backroom

During National Small Business Week, the City of Marietta Office of Economic Development partnered with the Marietta Business Association to host a series of events for and about small businesses. In particular, Tuesday's roundtable about "Managing the Backroom" provided great insights into ideas many small businesses should, but too often don't, consider.

Training and Controls

While small businesses are often celebrated for their flexibility, established procedures and controls can prepare businesses for "not if, but when" scenarios. Such events can include EEOC charges by employees, loss of proprietary information, and theft. By integrating some of the following systems, small businesses can better navigate hazards and continue to run smoothly.

- **Provide and update a well-drafted employee handbook.** It is not enough to go online for this. Your handbook codifies what you expect from your employees. It should be unique to your business and change as your business changes. It may even be beneficial to have your handbook reviewed by a lawyer as it may be used as evidence for (or against) you.
- **Train management on what isn't acceptable in the workplace.** It isn't enough to let "common sense" dictate your policies. While managers might like to joke with staff, it is critical that managers know when to stop.
- **Plan for common scenarios.** What will happen to the business if your primary salesperson leaves? What will happen if a business partner becomes ill or dies? Do you have dual controls in place to catch someone who is stealing from within? Ask questions regarding common issues like these before you find yourself in that situation.

Cybersecurity for Small Businesses

Given how much we depend on technology, a significant amount of time was spent discussing how to manage this asset and the associated threats. Just as businesses install an alarm system for physical threats, businesses have to keep cybersecurity in mind. The theft of sensitive, digital property can leave businesses (and their customers) with losses greatly exceeding losses from any potential theft of physical property. To lessen your chances of becoming a victim of cyber theft, consider the following:

- **Don't let your work computer double as your personal computer.** By limiting the amount and type of access you have to the internet, you limit the number of access points attackers can use invade your privacy.
- **When picking business partners, ask if they are aware of the risks of cyberattacks and what they're doing to combat it.** Cybersecurity (and business) is a 2 way street. Just as your customers might provide you with



2015 National Small Business Week



sensitive information (bank accounts, addresses, social security number, etc), your business provides similar information and access to your business partners.

- **Never click on an email attachment unless a) you know the sender and b) you are expecting the attachment.** Attackers become more and more sophisticated as days pass. While everyone knows to avoid emails from strangers, be cautious even when opening emails from friends and family as their emails may have been hacked.

Running a business will present plenty of opportunities for you to be flexible and adapt, but reduce and manage the risks. When facing these challenges, never forget to **consult with your team of experts.** Whether paid consultants or acquaintances from networking events, build your team to your weaknesses so you can be ready. In the words of American statesman and small business owner Benjamin Franklin, **“an ounce of prevention is worth a pound of cure.”**

Special thanks to our discussion participants including Mary Karras, Senior Vice President for the Bank of North Georgia, Evan Rosen of Jackson Lewis P.C., Antonio Barrios from the Small Business Development Center, Dave Olsen of North Star Payroll, and Dr. Herb Mattord of Kennesaw State University.